CYBERBEVEILIGING VOOR KLEINERE ORGANISATIES

CISO-CHECKLIST: UW KLANTEN BESCHERMEN

KLANTEN EN MEDEWERKERS OP INDIVIDUEEL NIVEAU ADVISEREN OVER GEGEVENSBESCHERMING

☐ **Geef medewerkers en klanten de volgende persoonlijke richtlijnen om hun gegevens beter te beschermen:**

- Gebruik sterke wachtwoorden op alle persoonlijke en werkapparaten en overweeg het gebruik van een wachtwoordmanager.
- Houd besturingssystemen en andere software en applicaties op uw computers en mobiele apparaten up-to-date.
- Installeer antivirus-, anti-malware- en anti-ransomware-software die kwaadaardige programma's tegenhoudt, detecteert en verwijdert.
- Gebruik een firewallprogramma om onbevoegde toegang tot uw computer te voorkomen.
- Gebruik alleen beveiligingsproducten van gerenommeerde bedrijven. Lees beoordelingen uit computer- en consumentenbladen en overleg eventueel met de fabrikant van uw computer of besturingssysteem.
- Ga zorgvuldig om met gevoelige informatie. Stuur geen bankrekeningwachtwoorden of andere gevoelige gegevens van financiële accounts via niet-versleutelde e-mail.
- Denk goed na over waar en hoe u verbinding maakt met het internet om te bankieren of berichten met gevoelige persoonlijke gegevens te versturen.
- Open niet meteen e-mailbijlagen en klik niet op links in ongevraagde of verdachte e-mails. Stop. Denk na. Klik.
- Wees argwanend als iemand u onverwacht online of telefonisch contacteert en u om persoonlijke gegevens vraagt. Zelfs wanneer u met bekende adressen communiceert, doet u er goed aan zo min mogelijk persoonlijke gegevens via e-mail te delen.
- Vergeet niet dat geen enkele financiële instelling u zal e-mailen of bellen en om vertrouwelijke informatie zal vragen die ze al over u hebben.
- Ga ervan uit dat een verzoek om informatie van een bank waar u nog nooit een rekening hebt gehad frauduleus is.
- Controleer of een verdachte e-mail of een verdacht pop-upvenster legitiem is voordat u persoonlijke gegevens verstrekt. Let goed op het e-mailadres.

ACCOUNTS BEHEREN

☐ **Vraag klanten om sterke gebruikers-ID's en wachtwoorden te gebruiken om in te loggen op uw diensten. Adviseer hen niet hetzelfde wachtwoord te gebruiken als voor andere accounts.**

☐ **Gebruik directe verificatie, realtimeverificatie, verificatie door een testbetaling, identiteitsverificatie en/of out-of-wallet-vragen om na te gaan of het om echte klanten gaat en de kans op fraude te verminderen.**

☐ **Bied klanten idealiter tweeledige verificatie aan bij het inloggen op uw diensten.**

☐ **Controleer de gebruikersaccounts regelmatig op tekenen van fraude.**

GEGEVENS BESCHERMEN

- ☐ **Bedenk welke klantgegevens uw organisatie moet verzamelen om haar diensten uit te voeren, en verzamel bij voorkeur geen klantgegevens die daar niet voor nodig zijn.**
- ☐ **Stel beleid voor gegevensbewaring op en verspreid dit binnen de organisatie. Verwijder klantgegevens wanneer ze niet meer nodig zijn.**
- ☐ **Versleutel klantgegevens tijdens verzending en opslag.**
- ☐ **Stel gegevensbeveiligingsbeleid op om duidelijk te maken welke methoden voor gegevensoverdracht worden goedgekeurd of beperkt en om te specificeren wat acceptabel is voor alle medewerkers bij hun omgang met klantgegevens. Zorg ervoor dat alle medewerkers op de hoogte zijn van dit beleid en zich eraan houden; evalueer het beleid geregeld en werk het waar nodig bij.**

OPENBARE WEBAPPLICATIES BEVEILIGEN

- ☐ **Implementeer HTTPS in de webapplicatie(s) van uw organisatie en leid al het HTTP-verkeer om naar HTTPS.**
- ☐ **Maak op uw website(s) gebruik van een contentbeveiligingsbeleid.**
- ☐ **Schakel koppeling van openbare sleutels op uw website(s) in.**
- ☐ **Zorg ervoor dat uw publieksgerichte webapplicatie(s) nooit cookies gebruiken om zeer gevoelige of kritieke klantinformatie (zoals wachtwoorden) op te slaan en dat de cookies niet te lang blijven staan.**
- ☐ **Versleutel eventueel de informatie die is opgeslagen in de cookies die u plaatst.**
- ☐ **Overweeg om de beveiliging van uw publieksgerichte webapplicatie(s) minimaal eenmaal per jaar te laten beoordelen door een penetratietestservice.**

MEDEWERKERS TRAINEN

- ☐ **Leer uw medewerkers verantwoordelijkheid op zich te nemen en reik strategieën aan om menselijke fouten waarbij klantgegevens zouden kunnen worden blootgesteld zoveel mogelijk te voorkomen. Adviseer ze dus om:**
  - Hun toegang tot en doorgifte van klantgegevens tot een minimum te beperken tot wat nodig is om hun taken uit te voeren,
  - Sterke beveiligingspraktijken toe te passen op alle apparaten en accounts waarop klantgegevens worden verwerkt door sterke wachtwoorden en tweeledige verificatie te gebruiken, software bijgewerkt te houden en niet op verdachte links te klikken, en
  - Mogelijke interne of externe beveiligingsincidenten, dreigingen of verkeerde verwerking van gegevens aan het technisch personeel van uw organisatie en/of hoger management te melden.
- ☐ **Zorg ervoor dat uw werknemers documenten waarin ze toezeggen zich te zullen houden aan de beleidsregels inzake gegevensbescherming en beveiliging van uw organisatie begrijpen en hebben ondertekend.**

KLANTEN INFORMEREN

☐ **Besteed aandacht aan de regelgeving die voor uw organisatie van toepassing is als het gaat om de omgang met gegevensinbreuken van klanten zodat u weet wat de regels zijn als zich incidenten voordoen.**

☐ **Wanneer uw organisatie kennis krijgt van een geval van onbevoegde toegang tot gevoelige klantinformatie, stel dan snel een onderzoek in om te bepalen hoe groot de kans is dat de informatie is of zal worden misbruikt. Volg de beste praktijken op het gebied van kennisgeving en breng de betrokken klant(en) zo snel mogelijk op de hoogte met:**

- Een algemene beschrijving van het incident en de informatie waarop de gegevensinbreuk betrekking heeft;
- Een telefoonnummer voor meer informatie en hulp;
- Een herinnering om de komende 12 tot 24 maanden "waakzaam te blijven";
- Een aanbeveling om gevallen van vermoede identiteitsdiefstal onmiddellijk te melden;
- Een algemene beschrijving van de stappen die de financiële instelling heeft genomen om de informatie te beschermen tegen verdere onbevoegde toegang of onbevoegd gebruik;
- Contactgegevens van kredietinformatiebureaus; en
- Alle overige informatie die uw organisatie overeenkomstig de regelgeving moet verstrekken.

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

CarnegieEndowment.org

THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP
SWIFT INSTITUTE
FS-ISAC
Standard Chartered
CYBER READINESS INSTITUTE
GLOBAL CYBER ALLIANCE
ICBA Independent Community Bankers of America®